NFC for Free Rides and Rooms (on your phone)

Presented by:
Corey Benninger
Max Sobell

EUSecWest 2012

PREVIEW DECK
(Not for distribution)

NOTICES

NOTICE
NOT RESPONSIBLE FOR CUTS, BRUISES, LOSS OF PROPERTY AND OR LIFE
SEPTA

Affected systems we know of have been contacted in Dec 2011 and March 2012, given detailed information and remediation recommendations

NFC Transit Overview

- Who's using it
  - Stateside
    - Transit (SF, Boston, DC, Seattle, NJ, Salt Lake City, Chicago, Philadelphia). NOT NEW YORK!
    - Known cities we've contacted: NJ Path, SF Muni
  - Overseas implementations
    - Malaysia, Hong Kong, London, Germany, Dubai, Madrid, etc.
- Benefits for Transit Agencies
  - Faster
  - Auto refill
  - Track riders

What's in a Tag

- Coil Antenna
  - powered by reader
    - inductive-coupling
- Integrated Circuit "IC"
  - Logic
    - Command set
  - Memory
    - 64 bytes to 8KB

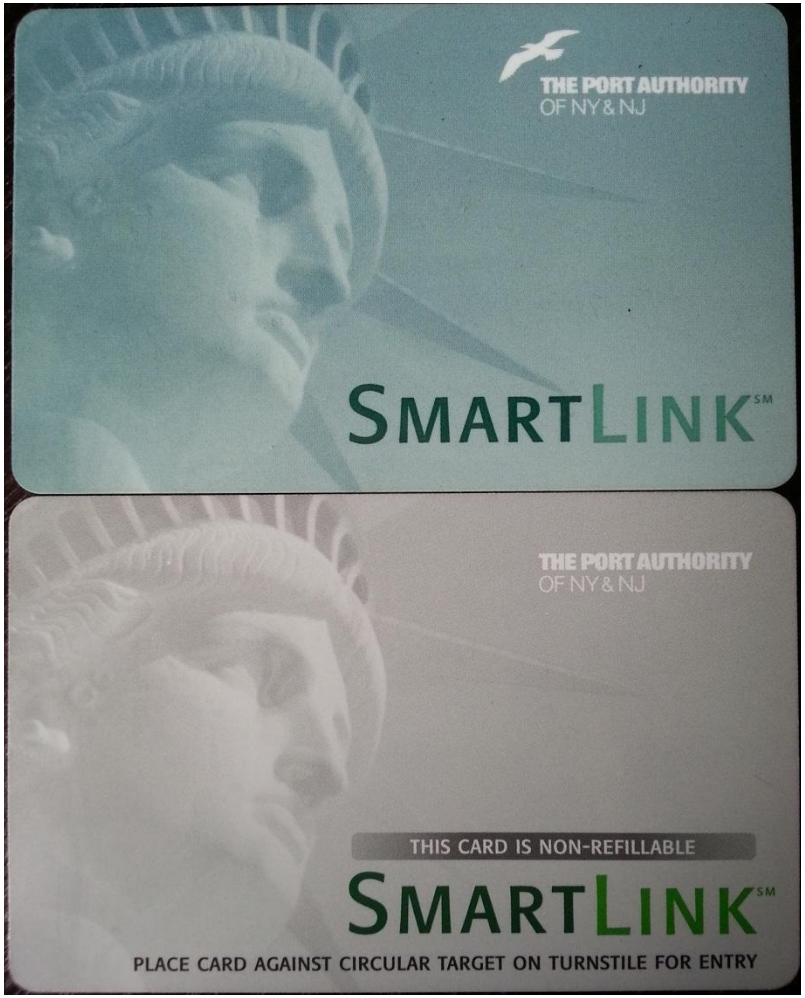
What's a Reader

- RFID @ 13.56 MHz
  - ISO 14443-1:4
  - Powers passive tags
    - Short range
    - Initialization and anti-collision
- Sends commands to cards
  - Read or Write commands
    - Typically to a sector
  - Slow baud rate
    - 106 kbps to 848 kbps

NFC Readers

- Many phone are also NFC Readers
  - Android (Nexus S, 7, Galaxy S3), Blackberry (Bold 9930), Nokia, Windows Phone…
  - Can emulate tags too
    - More on that later…

RFID Transit Cards


THE PORT AUTHORITY OF NY & NJ
SMARTLINK SM
THE PORT AUTHORITY OF NY & NJ
THIS CARD IS NON-REFILLABLE
SMARTLINK SM
PLACE CARD AGAINST CIRCULAR TARGET ON TURNSTILE FOR ENTRY

- Top:
  - **Mifare DESFire**
  - Supports Access Control
    - Separate read/write keys
- Bottom:
  - **Mifare Ultralight**
  - No Access Control

RFID Transit Cards

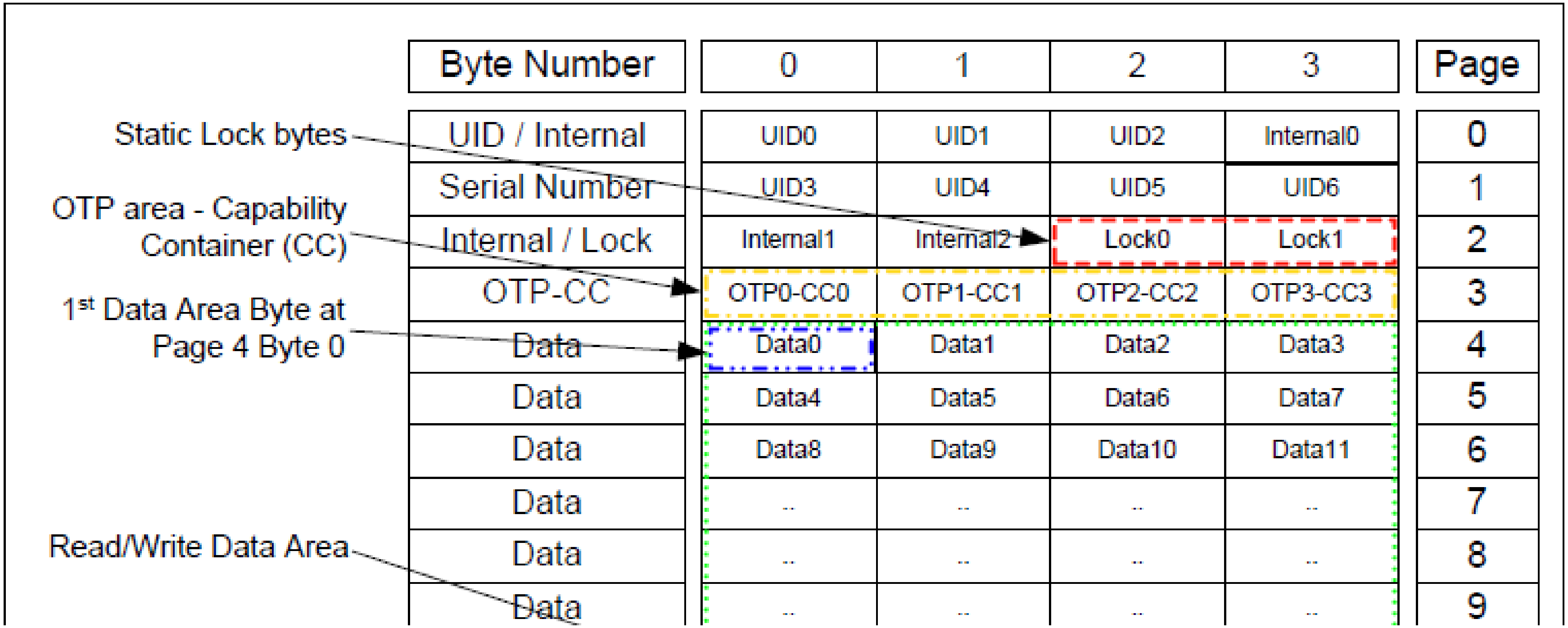
Mifare Ultralight

Mifare DESFire

Types of Tags

- Choosing the right type of tag is IMPORTANT!!!
  - Not all tags support the same features
    - Might need to be used in different ways

Ultralight breakdown



Byte Number	0	1	2	3	Page
UID / Internal	UID0	UID1	UID2	Internal0	0
Serial Number	UID3	UID4	UID5	UID6	1
Internal / Lock	Internal1	Internal2	Lock0	Lock1	2
OTP-CC	OTP0-CC0	OTP1-CC1	OTP2-CC2	OTP3-CC3	3
Data	Data0	Data1	Data2	Data3	4
Data	Data4	Data5	Data6	Data7	5
Data	Data8	Data9	Data10	Data11	6
Data	..	..	..	..	7
Data	..	..	..	..	8
Data	..	..	..	..	9

Static Lock bytes

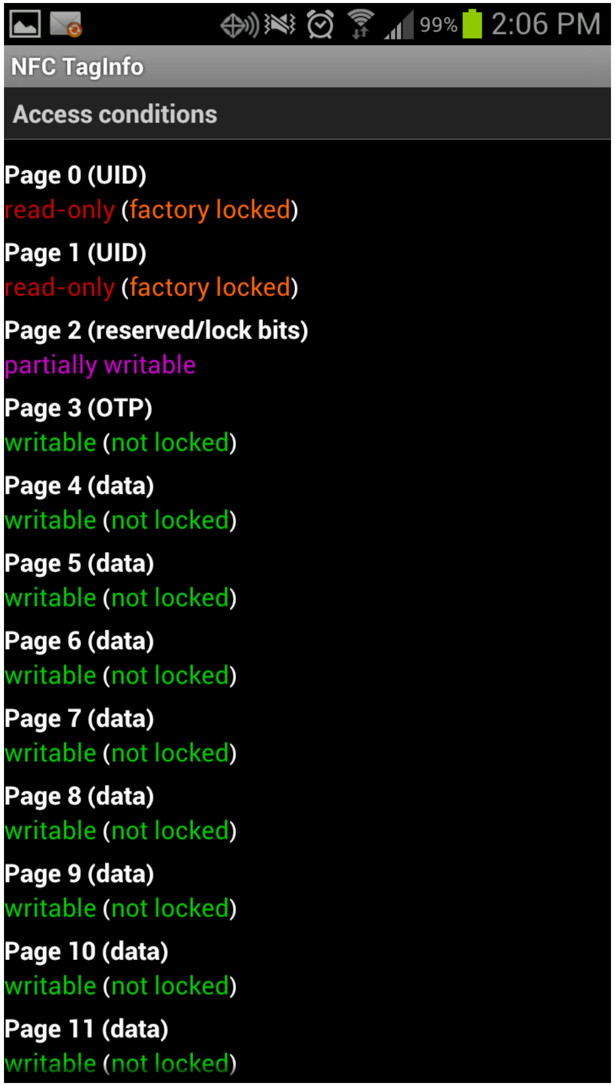
OTP area - Capability Container (CC)

1st Data Area Byte at Page 4 Byte 0

Read/Write Data Area

- **Ultralight Memory Layout - AN1303 document from NXP**
  - Read/Write data area starting at Page 4 can be altered by all users

Analyzing Cards



NFC TagInfo

Access conditions

Page 0 (UID)
read-only (factory locked)

Page 1 (UID)
read-only (factory locked)

Page 2 (reserved/lock bits)
partially writable

Page 3 (OTP)
writable (not locked)

Page 4 (data)
writable (not locked)

Page 5 (data)
writable (not locked)

Page 6 (data)
writable (not locked)

Page 7 (data)
writable (not locked)

Page 8 (data)
writable (not locked)

Page 9 (data)
writable (not locked)

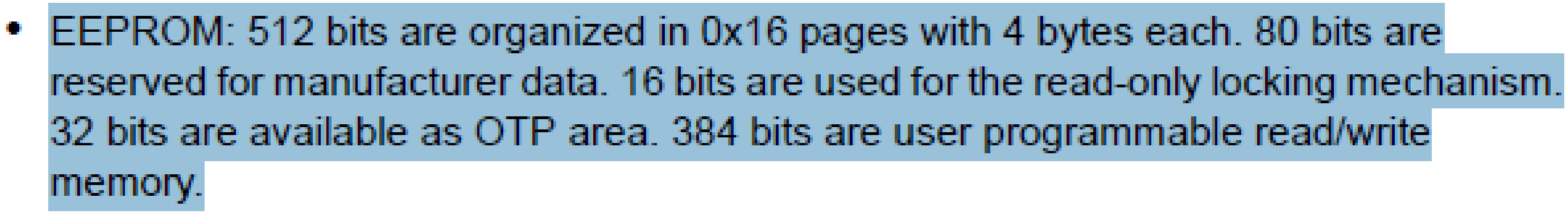
Page 10 (data)
writable (not locked)

Page 11 (data)
writable (not locked)

View a Mifare Ultralight tag with Android

- NFC TagInfo
  - NFC Research Lab Hegenberg
- Permissions are color coded
  - Red locked pages
  - Green not locked

No Access Ctrl, but OTP



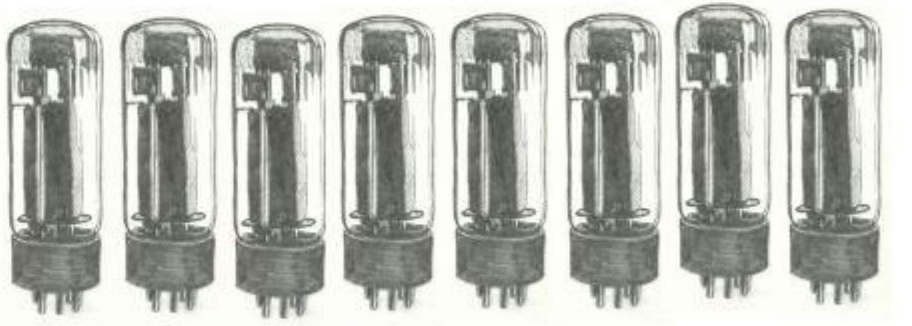
- EEPROM: 512 bits are organized in 0x16 pages with 4 bytes each. 80 bits are reserved for manufacturer data. 16 bits are used for the read-only locking mechanism. 32 bits are available as OTP area. 384 bits are user programmable read/write memory.

OTP = One Time Programmable

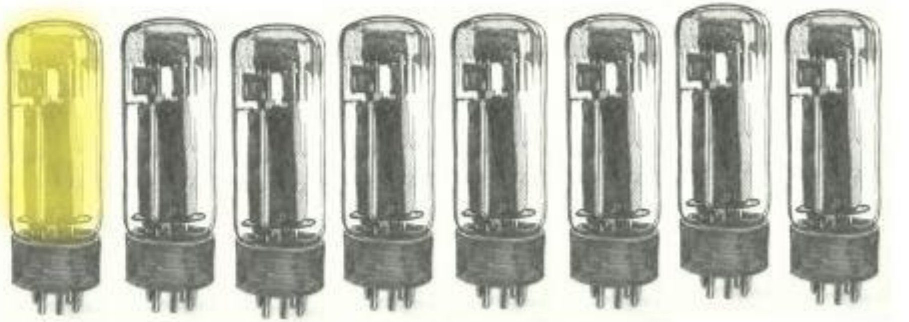
- Area in Page 3 which bits can be set once (1b), but never unset (0b)
- This area was envisioned to be used for ticketing systems (if all tickets are of equal value). Each 32 bits can represent one "ride". A time of purchase, the correct value of "rides" left is set.
- The amount of "rides" is decremented each time and can not be reused once all are gone.

OTP – flipping the bits

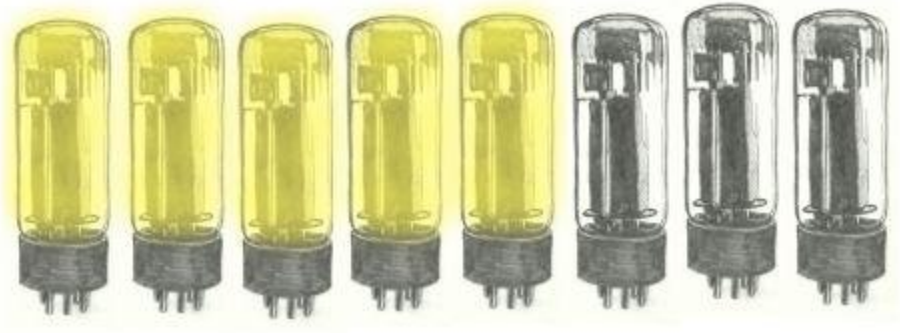
8 “rides” remain
(0x00)



7 “rides” remain
(0x80)

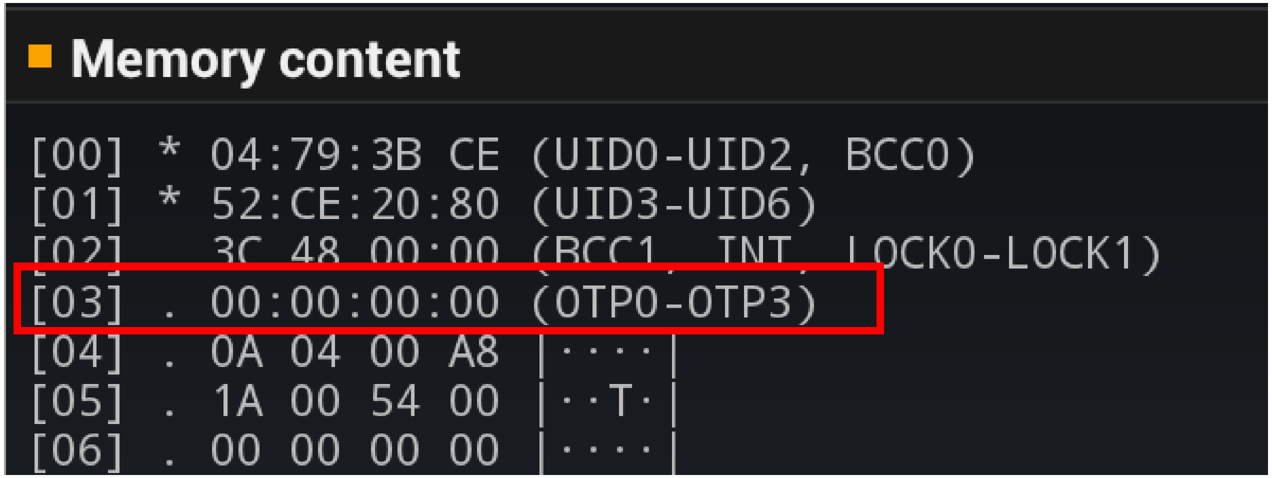


3 “rides” remain
(0xF8)



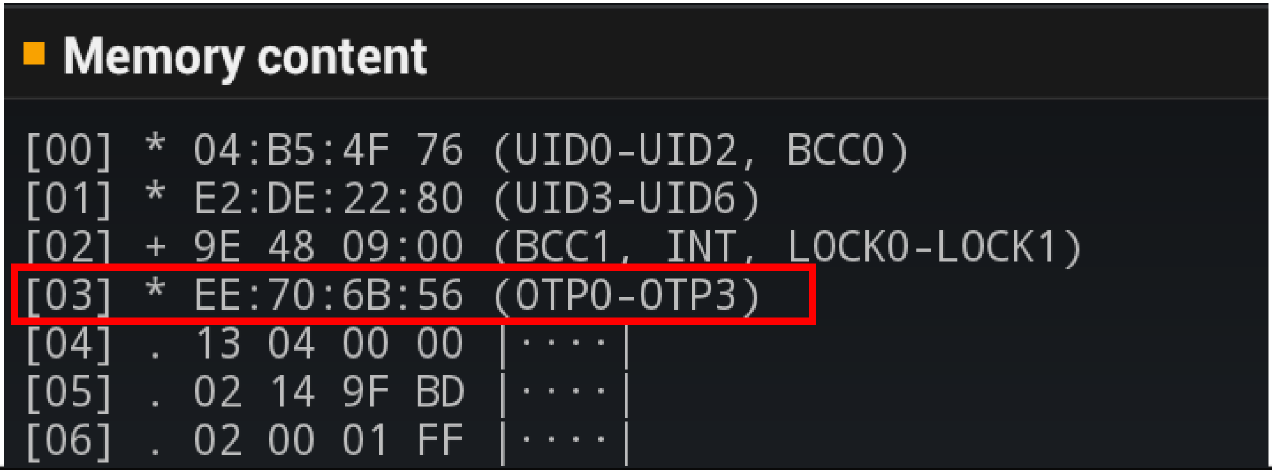
OTP on Transit Cards

- East Coast vs West Coast



Memory content

```
[00] * 04:79:3B CE (UID0-UID2, BCC0)
[01] * 52:CE:20:80 (UID3-UID6)
[02]   3C 48 00:00 (BCC1, INT, LOCK0-LOCK1)
[03] . 00:00:00:00 (OTP0-OTP3)
[04] . 0A 04 00 A8 |····|
[05] . 1A 00 54 00 |··T·|
[06] . 00 00 00 00 |····|
```



Memory content

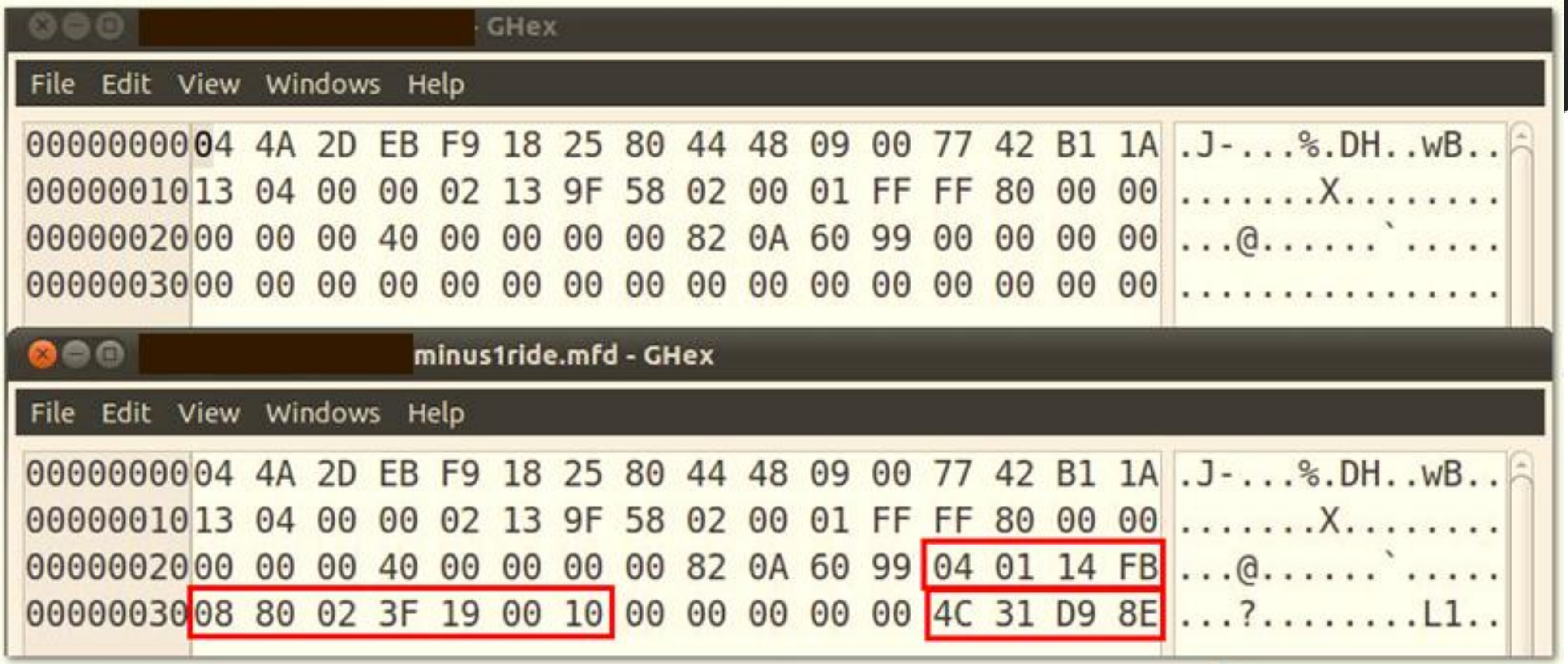
```
[00] * 04:B5:4F 76 (UID0-UID2, BCC0)
[01] * E2:DE:22:80 (UID3-UID6)
[02] + 9E 48 09:00 (BCC1, INT, LOCK0-LOCK1)
[03] * EE:70:6B:56 (OTP0-OTP3)
[04] . 13 04 00 00 |····|
[05] . 02 14 9F BD |····|
[06] . 02 00 01 FF |····|
```

OTP on Transit Cards

- Looking at the OTP settings alone won't verify is a system is vulnerable or not
  - Positive Signs of doing it right
    - If OTPs are set to a logical value at time of purchase
    - OTPs change after card is used

Raw Data Dumps

Transit card data



[redacted] - GHex
File Edit View Windows Help

```
00000000 04 4A 2D EB F9 18 25 80 44 48 09 00 77 42 B1 1A  .J-...%.DH..wB..
00000010 13 04 00 00 02 13 9F 58 02 00 01 FF FF 80 00 00  .......X........
00000020 00 00 00 40 00 00 00 00 82 0A 60 99 00 00 00 00  ...@....[redacted]`.....
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

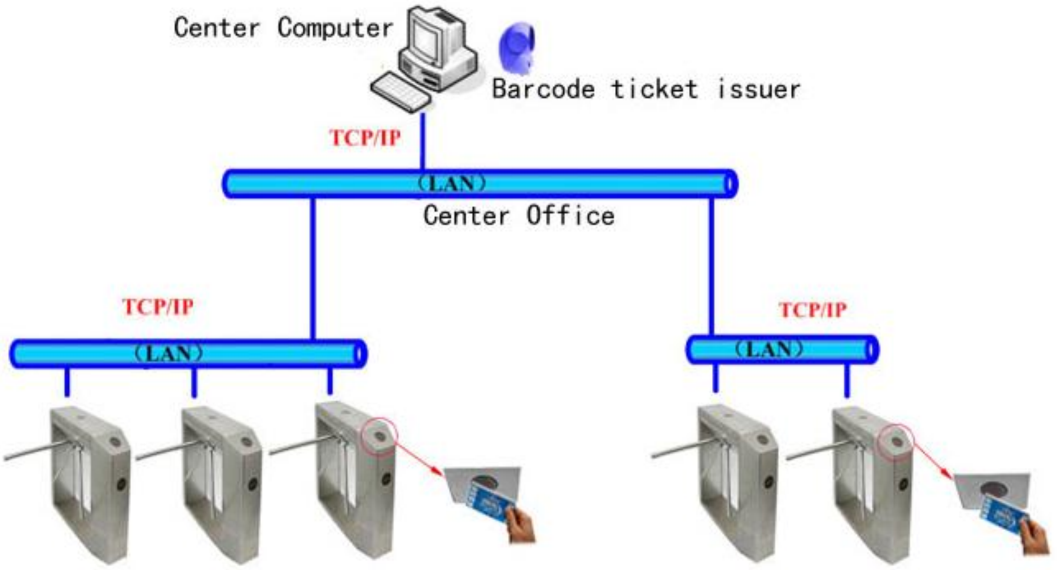
[redacted] minus1ride.mfd - GHex
File Edit View Windows Help

```
00000000 04 4A 2D EB F9 18 25 80 44 48 09 00 77 42 B1 1A  .J-...%.DH..wB..
00000010 13 04 00 00 02 13 9F 58 02 00 01 FF FF 80 00 00  .......X........
00000020 00 00 00 40 00 00 00 00 82 0A 60 99 04 01 14 FB  ...@....[redacted]`.....
00000030 08 80 02 3F 19 00 10 00 00 00 00 00 4C 31 D9 8E  ...?........L1..
```

- Top Screen: Card data PRIOR to first use
- Bottom Screen: Card data AFTER first use

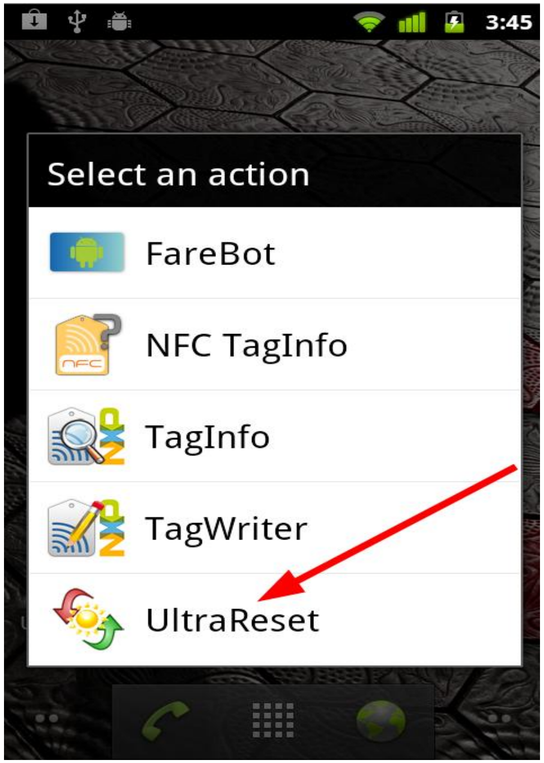
Vulnerable?

- System could be validating card on backend systems
  - Remote server could keep count of card usage



Vulnerable?

- Only way to test your system…
  - is to test your system.



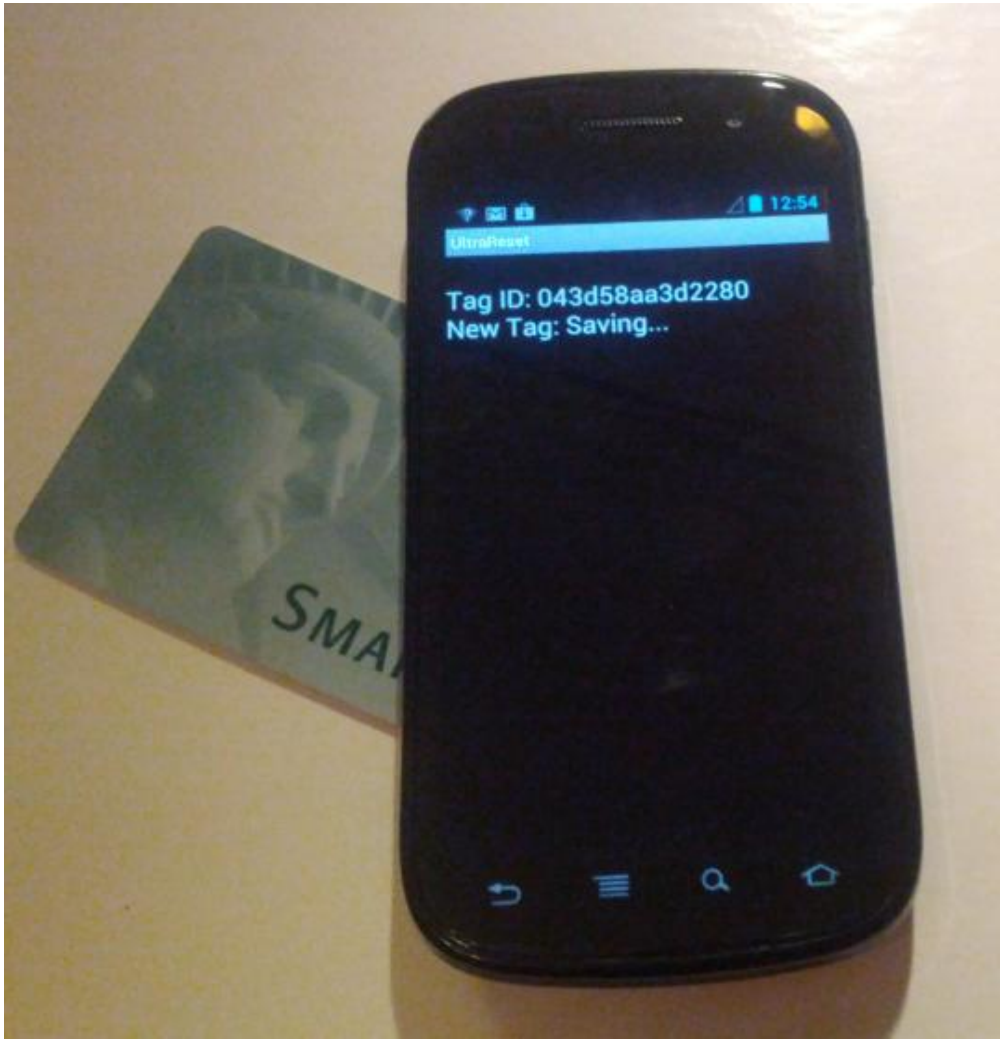
Select an action

- FareBot
- NFC TagInfo
- TagInfo
- TagWriter
- UltraReset

UltraReset

- Works on any Android device with NFC
  - (2.3.3 or later)
- Uses standard NFC API Calls

UltraReset



```
Tag ID: 043d58aa3d2280
New Tag: Saving...
```

- Step 1
  - – Save card data on to phone
    - Pages 3 to 15 are saved to phone

<u>Example Card</u>
Rides left on card: 10

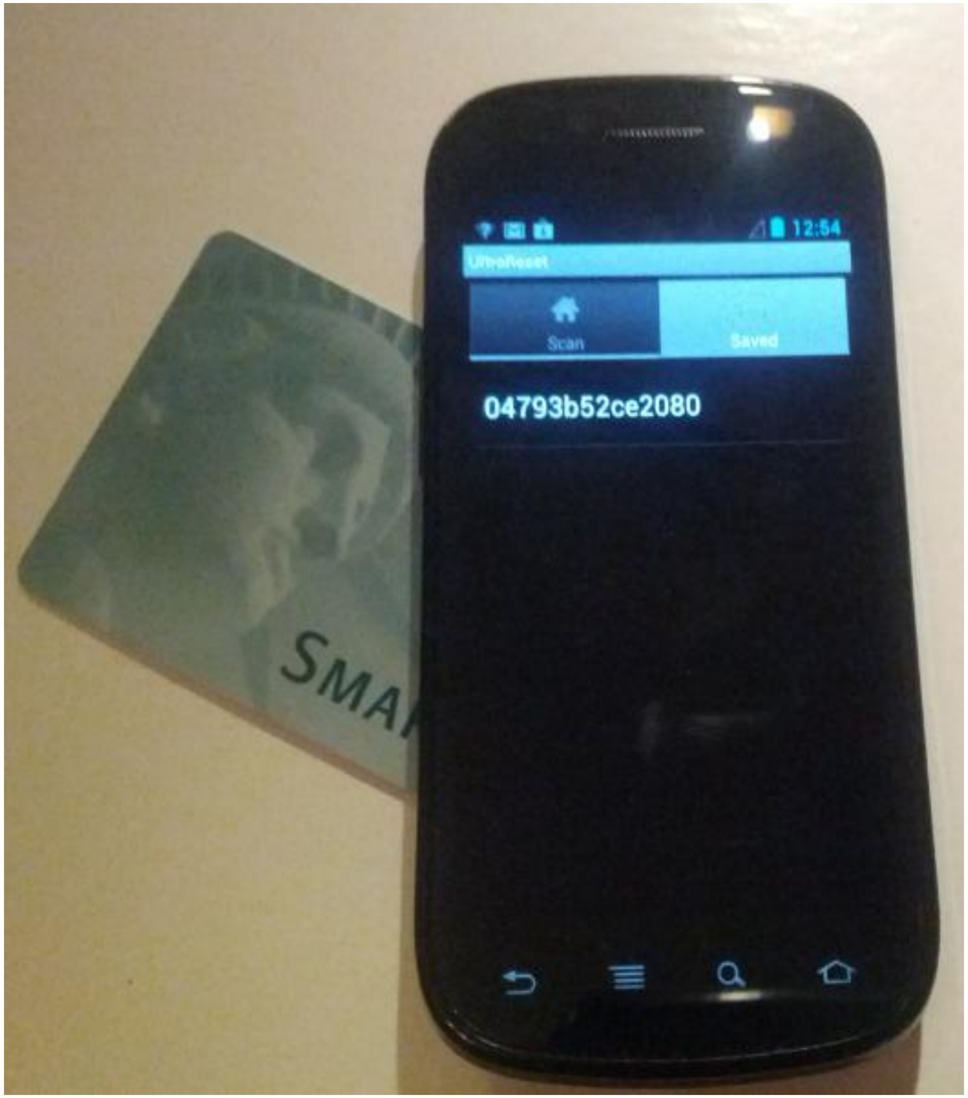
UltraReset

- Step 2
  - Use transit card

Example Card

Rides left on card: 8

UltraReset



04793b52ce2080

- Step 3
  - Write original data back to card
    - Pages 3 to 15 are reset to originally saved data from the phone

Example Card

Rides left on card: 10

Got Issues

Flaw in the "Single" ride or temporary use cards

- Rider is typically not charged directly for the card
- However, transit system may have spent $$$
- Wholesale $0.05 to $0.20 per card
- Cards designed to be disposable
  - should not be "refillable"

Ultralight Upgrade

- Mifare Ultralight
  - Envisioned for ticketing purposes
  - Just fine for events
    - Enter once, that’s all you want. Easy to track UIDs.
  - Received upgrade: Ultralight C
    - Has same OTP bits, now called “one way counter”
    - Mifare’s customer education?
    - C’s also support access control

Contact

- Corey Benninger (corey@intrepidusgroup.com)
- Max Sobell (max.sobell@intrepidusgroup.com)